REMARKS

Claims 1-12 are pending, with claims 1 and 6 being in independent form.

In the Office Action, FIGS. 1-4 are objected to for failing to include a "Prior Art" legend. The Applicants have amended the figures to add the required legend to address the Office's concern. Accordingly, reconsideration and withdrawal of the objection is respectfully requested.

Claims 1-12 stand rejected for indefiniteness. The Office asserts that the phrase "authentication ciphering offset" is not a phrase recognized by persons skilled in the art and is indefinite because the specification does not clearly define the phrase. The Applicants respectfully disagree.

First, the term ACO is a term that is recognized by persons of ordinary skill in the art, especially those familiar with Bluetooth communication systems. Second, the original specification describes on page 3, line 22, to page 4, line 3, that:

> To further increase difficulties for a malicious unit, the creation of the encryption key is dependant not only on the link key, but also on a number that is denoted "Authentication Ciphering Offset" (ACO). The ACO is a number that is created for every call of the function that generates the SRES. If two units switch on encryption with different ACOs, their respective generated encryption key will differ even if they use the same link key.

The Applicants respectfully assert that this introductory definition of an ACO, together with detailed description of the use the ACO throughout the written description and drawings, makes clear the meaning of the term.

Nevertheless, the Applicants have amended the Background Section to recite the section included in the most recent Bluetooth specification that describes this term in greater detail. Accordingly, the Applicants respectfully request that the Office reconsider and withdraw the indefiniteness rejection.

Turning to the art rejections, claims 1-10 have been rejected for anticipation by U.S. Patent No. 5,148,007 to Kruse. Claims 11-12 stand rejected for obviousness over Kruse in view of U.S. Patent No. 6,577,633 to Kunito et al. ("Kunito"). The Applicants believe the pending claims are allowable over the cited documents for the following reasons.

Anticipation requires that every feature of the claimed invention be shown in a single prior document. *In re Paulsen*, 30 F.3d 1475 (Fed. Cir. 1994); *In re*

Robertson, 169 F.3d 743 (Fed. Cir. 1999). The pending claims positively recite features that are not described in the cited document.

For example, claim 1 defines a method of generating an ACO in a communication device that includes "generating the ACO as a function of one or more parameters, wherein at least one of the one or more parameters is derived from earlier-computed values of the ACO". Based on the discussion above, the plain meaning of the ACO being generated should be clear to those skilled in the art. The Office asserts that claim 1 reads on Kruse's first and second authorization parameters AP1 and AP2. The Applicants respectfully disagree.

The Applicants describe in the paragraph beginning at page 2, line 27, of the application that:

> The authentication procedure in Bluetooth follows a challenge-response scheme. In short, the verifier generates a challenge in the form of a random number (denoted herein as AU_RAND), that is sent to the claimant. Upon receiving this challenge, the claimant computes a signed response (denoted herein as SRES), that is sent back to the verifier. The verifier can independently compute what the response ought to be (denoted herein as SRES'), given the challenge and the shared secret link key used by the two Bluetooth units. If the received SRES equals the computed SRES', the authentication is considered successful. If, on the other hand, these two numbers differ, the claimant failed to prove its identity.

The Applicants further describe that, separate from the concept of authentication, if an application at some point requires data confidentiality, encryption can be used. Encryption can require the use of a shared secret encryption key that is typically different from, but derived from, the link key used for authentication. *See* p. 3, ll. 13-21.

As discussed above, in Bluetooth, the creation of an encryption key can be dependant both on the link key and on the ACO. The ACO is a number that is created for every call of the function that generates the SRES used for authentication. Consequently, if two units attempt to share data that is encrypted with different ACOs, their respective generated encryption keys will differ from one another, even if the units use the same link key. Importantly, unlike the random number AU_RAND, sent by a verifier to a claimant under a challenge-response scheme, and the signed response SRES, sent from the claimant back to the verifier, the generated ACOs are not shared between units.

In contrast, Kruse's V1, V2 can correspond to the Applicants' AU_RAND, and Kruse's AP1, AP2 can correspond to the Applicants' SRES, SRES' described in the application. In the cited portion relied upon in the Office Action, Kruse describes that that "mutually transmitted first and second authorization parameters AP1, AP2 are then advantageously used for generating a variable starting value for a new random number". Accordingly, the generation of Kruse's random number requires the mutual exchange of the first and second authorization parameters AP1, AP2 between the devices.

The plain meaning of an ACO, as understood by those of ordinary skill in the art, is a number used for generation of an encryption key that is neither exchanged, nor representative of numbers exchanged, between devices sharing information. Since Kruse's authorization parameters AP1, AP2 represent neither of these inherent features of claim 1, which recites a method of generating an ACO, the claim is believed not to be anticipated by Kruse as the Office asserts. The same can be said for claim 6, which recites features substantially similar to claim 1.

Accordingly, claims 1 and 6 are believed to be allowable for least the above reasons. Moreover, the remaining claims, which depend either directly or indirectly from one of claims 1 and 6, are believed to be allowable over Kruse for at least these same reasons.

In addition, claims 2 and 7 are considered allowable over Kruse for the following reasons. Claims 2 and 7 recite "generating the ACO as a function of one or more parameters comprises generating a *k*th value, X_k from one or more of the parameters, and applying a commutative binary operation between X_k and a previous value, ACO_{k-1}",. The Office asserts that Kruse discloses the recited features at column 3, lines 1-16, in conjunction with the generation of the random number V2, which the Office asserts is equivalent to the recited X_k. The Applicants respectfully disagree.

The X_k recited in claims 2 and 7 can be used in generating the ACO. X_k is not equivalent to V2 (or V1) as the Office asserts. For example, unlike V2 (and V1), X_k is not revealed to the other side as are Kruse's public random numbers V1, V2 that are mutually transmitted during an authentication procedure. Accordingly, claims 2 and 7 are considered to be allowable for this reason as well.

Regarding claims 3 and 8, these claims recite generating a *k*th value of the ACO as a running sum in accordance with the equation $ACO_k = X_k \oplus ACO_{k-1} = \sum_{i=1}^{k} X_i$, where X_i is generated as a function of the one or more parameters excluding the at least one of the one or more parameters that is derived from earlier-computed values of the ACO, The Office again asserts that the claim reads on Kruse's generation of a random number using AP1 and V2. But as discussed above, since AP1 is not equivalent to the recited ACO and since V2 is not equivalent to the recited X_k, the claim does not read on Kruse's method of generating a random number described in column 3, lines 1-16, as the Office asserts. Accordingly, claims 3 and 8 are believed to be allowable over Kruse for these reasons as well.

For the foregoing reasons, it is believed this application is in condition for allowance and an early Notice thereof is earnestly solicited. If any questions remain, the Examiner is invited to phone the undersigned at the below-listed number.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: _____
Stephen J. Tytran
Registration No. 45,846

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

Date: July 14, 2004

Attachments: Replacement Drawing Sheets (4)

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date of Deposit: July 14, 2004

_____
Stephen J. Tytran